Fermat'n pieni lause

Heikki Pitkänen

Matematiikan kandidaatintutkielma

Jyväskylän yliopisto
Matematiikan ja tilastotieteen laitos
Kevät 2009

Sisältö

Johdanto 3
1. Fermat'n pieni lause 3
2. Pseudoalkuluvut ja Carmichaelin luvut 4
3. Eulerin funktio, $\phi(n)$ 5
4. Eulerin lause 6
5. Eulerin funktion arvo 6
6. Yksiköiden ryhmän U_n syklisyys 8
7. Sovelluksia 9
Kirjallisuutta 12

Johdanto

Tässä työssä tutkimme Fermat'n pientä lausetta, Eulerin funktiota ja yksiköiden ryhmää $U_n \subset Z_n$. Toteamme myös, että on olemassa lukuja, jotka toteuttavat Fermat'n lauseen kaavan olematta kuitenkaan alkulukuja. Todistamme lisäksi Fermat'n lausetta yleisemmän tuloksen. Lopuksi perehdymme hieman Eulerin ja Fermat'n lauseiden sovelluksiin salausmenetelmissä. Oletuksena on, että lukijalla on perustiedot algebrasta ja erityisesti ryhmäteoriasta.

1. Fermat'n pieni lause

Määritelmä 1. Kokonaislukua $p > 1$ kutsutaan *alkuluvuksi*, jos se on jaollinen ainoastaan luvulla 1 ja itse luvulla p.

Määritelmä 2. Määritellään ekvivalenssirelaatio $\equiv \pmod p$:

$$a \equiv b \pmod p \iff b = kp + a \ jollain \ k \in \mathbb{Z}.$$

Määritelmä 3. Ekvivalenssirelaatiota $\equiv \pmod p$ vastaavaa tekijäjoukkoa $\mathbb{Z}/_{\equiv \pmod p}$ merkitään $\mathbb{Z}_p := \{[0], [1], \ldots, [p-1]\}$.

Ekvivalenssiluokka $[a] \in \mathbb{Z}_p$ koostuu siis niistä luvuista b, jotka jättävät jakojäännökseksi luvun a jaettaessa luvulla p.

Esimerkki 4. a) $21 \equiv 16 \equiv 1 \pmod 5$, sillä $16 = 3 \cdot 5 + 1$ ja $21 = 4 \cdot 5 + 1$
b) $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$
c) Olkoon $[3] \in \mathbb{Z}_5$. Tällöin $-7, -2, 3, 8, 13, \ldots \in [3]$

Lause 5. *Tekijälaskutoimitukset "$\cdot$" ja "$+$" ovat yhteensopivia ekvivalenssirelaation* $\equiv \pmod p$ *kanssa.*

Todistus. Olkoon $a \equiv a' \pmod p$ ja $b \equiv b' \pmod p$. Siis on olemassa $r, s \in \mathbb{Z}$ siten, että $a + rp = a'$ ja $b + sp = b'$. Tutkitaan tuloa $a' \cdot b'$:

$$a' \cdot b' = (a + rp)(b + sp) = ab + asp + brp + srp^2 \equiv a \cdot b \pmod p$$

Siis $a' \cdot b' \equiv a \cdot b \pmod p$. Tekijälaskutoimitus "$\cdot$" on siten yhteensopiva. Tutkitaan summaa $a' + b'$:

$$a' + b' = (a + rp) + (b + sp) = a + b + (r + s)p \equiv a + b \pmod p$$

Siis $a' + b' \equiv a + b \pmod p$. Myös tekijälaskutoimitus "$+$" on yhteensopiva. □

Ennen Fermat'n pienen lauseen todistusta palautamme mieleen muutaman algebrasta tutun määritelmän ja lauseen sekä todistamme toisen tarvittavan tuloksen:

Määritelmä 6. Olkoon äärellisen ryhmän G neutraalialkio e. Tällöin alkion $a \in G$ *aste* on pienin luonnollinen luku k, jolle $a^k = e$ ja merkitään $\#a = k$. Ryhmän G *aste* on sen alkioiden lukumäärä ja merkitään $\#G$.

Määritelmä 7. Ryhmä G on *syklinen*, jos on olemassa $a \in G$ siten, että

$$G = \{a^k : k \in \mathbb{N}\} =: \langle a \rangle.$$

Sanotaan, että alkio a *virittää ryhmän* G.

Lause 8 (Lagrangen lause)**.** *Olkoon G äärellinen ryhmä, ja olkoon $H \subset G$ ryhmän G aliryhmä. Tällöin:*

$$\#G = \#(G/H)\#H = \#(H\backslash G)\#H.$$

Siis $\#G = k\#H$ jollain $k \in \mathbb{N}$.

Määritelmä 9. Kahden luvun $a, b \in \mathbb{N}$ *suurin yhteinen tekijä* k on on suurin kokonaisluku, joka jakaa luvut a ja b, siis $k \mid a$ ja $k \mid b$. Käytetään merkintää: $\text{syt}(a, b) = k$.

Lemma 10. *Jos* $\text{syt}(a, p) = d$*, yhtälöllä* $ax \equiv d \pmod{p}$ *on ratkaisu.*

Todistus. Jos $\text{syt}(a, p) = d$, niin joillakin $r, s \in \mathbb{Z}$ on voimassa Bezout'n yhtälö: $ar + ps = d$. Siis $ar = -ps + d$ ja siten $ar \equiv d \pmod{p}$. Yhtälöllä on siis ratkaisu r. □

Lause 11 (Fermat'n lause)**.** *Jos p on alkuluku ja $p \nmid a$ niin $a^{p-1} \equiv 1 \pmod{p}$.*

Todistus. Koska p on alkuluku ja $p \nmid a$ niin $a \not\equiv 0 \pmod{p}$. Tällöin jakojäännösten luokkien joukko $\mathbb{Z}_p^* = \{[a] \in \mathbb{Z}_p : p \nmid a\} = \{[1], [2], \ldots, [p-1]\}$ varustettuna tulolla muodostaa ryhmän: Selvästi tulo on assosiatiivinen, neutraalialkiona $[1]$. Tarkastettavaksi jää käänteisalkion olemassaolo kaikille $[a] \in Z_p^*$. Koska p on alkuluku, niin $\text{syt}(a, p) = 1$ ja yhtälöllä $ax \equiv 1 \pmod{p}$ on lemman 10 perusteella ratkaisu x, joten $[a]^{-1} = [x]$ on alkion $[a]$ käänteisalkio. Ryhmän $\mathbb{Z}_p^*$ alkion $[a]$ virittämä syklinen ryhmä $\langle [a] \rangle$ on ryhmän $\mathbb{Z}_p^*$ aliryhmä. Nyt Lagrangen lauseen nojalla: $\#\langle [a] \rangle \mid p-1$ eli jollain $k \in \mathbb{Z}$ on $p - 1 = k\#\langle [a] \rangle$. Koska alkion asteen määritelmän mukaan $[a]^{\#\langle [a] \rangle} = 1$, niin pätee:

$$[a^{p-1}] = [a]^{p-1} = [a]^{k\#\langle [a] \rangle} = [1]^k = [1]$$

Siispä $a^{p-1} \equiv 1 \pmod{p}$.

□

Seuraus 12. *Jos p on alkuluku, niin $a^p \equiv a \pmod{p}$.*

Todistus. Jos $p \nmid a$, niin Fermat'n lauseen perusteella $a^{p-1} \equiv 1 \pmod{p}$, joka kerrottuna molemmin puolin luvulla a antaa väitteen. Jos $p \mid a$, niin $p \mid a^p$, eli jos $a \equiv 0 \pmod{p}$, niin $a^p \equiv 0 \pmod{p}$. □

Esimerkki 13. Luvut 3 ja 5 ovat alkulukuja:

a) $2^3 = 8 \equiv 2 \pmod{3}$
b) $4^5 = 1024 \equiv 4 \pmod{5}$

2. Pseudoalkuluvut ja Carmichaelin luvut

Edellä esitetty yhtälö toteutuu kaikilla alkuluvuilla, mutta on olemassa myös lukuja, jotka toteuttavat yhtälön olematta kuitenkaan alkulukuja. Fermat'n lause antaa siis vain keinon testata, onko luku p mahdollisesti alkuluku. Yleensä aloitetaan testaamalla, päteekö luvulle $2^n \equiv 2 \pmod{n}$.

Määritelmä 14. Lukua n, joka ei ole alkuluku, mutta toteuttaa Fermat'n lauseen kaavan muodossa $2^n \equiv 2 \pmod{n}$ kutsutaan *pseudoalkuluvuksi.*

Esimerkki 15. Olkoon $a = 2$ ja $p = 341$. Huomataan, että $2^{10} = 1024 \equiv 1 \pmod{341}$. Tällöin $(2^{10})^{34} \equiv 1 \pmod{341}$ ja $2 \cdot 2^{340} = 2^{341} \equiv 2 \pmod{341}$. Nyt $p \nmid a$, ja $a^p = 2^{341} \equiv 2 \pmod{341}$. Kuitenkaan 341 ei ole alkuluku vaan $341 = 11 \cdot 31$.

Vaikka luku suoriutuisi edellisestä 2^n-testistä, se ei välttämättä ole alkuluku:

Määritelmä 16. Lukua n, joka ei ole alkuluku ja toteuttaa kaavan $a^n \equiv a \pmod{n}$ jokaisella kokonaisluvulla a kutsutaan *Carmichaelin luvuksi.*

Esimerkki 17. 561 on Carmichaelin luku. Todistus: Katso [2] sivut 76-77.

3. Eulerin funktio, $\phi(n)$

Kuten edellä huomattiin, Fermat'n lause pätee kaikille alkuluvuille, mutta myös joillekin kokonaisluvuille, jotka eivät ole alkulukuja. Johdamme seuraavaksi Fermat'n lausetta yleisemmän tuloksen koskemaan myös muita kuin alkulukuja. Tätä varten tarvitsemme muutaman määritelmän ja aputuloksen.

Määritelmä 18. Luokka $[a] \in \mathbb{Z}_n$ on *yksikkö*, jos on olemassa luokka $[b] \in \mathbb{Z}_n$, jolle pätee $[a][b] = [1]$. Tällöin luokka $[b]$ on luokan $[a]$ *käänteisalkio tulon suhteen.*

Lause 19. *Luokka $[a] \in \mathbb{Z}_n$ on yksikkö, jos ja vain jos* $\text{syt}(a, n) = 1$.

Todistus. Jos $[a] \in \mathbb{Z}_n$ on yksikkö, on olemassa $b, k \in \mathbb{Z}$ siten, että $ab = kn + 1$. Jos luvuilla a ja n olisi yhteinen tekijä $r > 1$, niin joillain $p, s \in \mathbb{Z}$ $prb = ksr + 1$, ja luvun r pitäisi jakaa luku 1. Siispä $\text{syt}(a, n) = 1$. Jos $\text{syt}(a, n) = 1$, niin joillain $u, v \in \mathbb{Z}$, $au + vn = 1$. Siis $au = 1 - vn \equiv 1 \pmod{n}$, joten $[u]$ on luokan $[a]$ käänteisalkio ja siten $[a]$ on yksikkö. □

Määritelmä 20. Merkitään joukon $\mathbb{Z}_n$ yksiköiden joukkoa U_n. Määritellään Eulerin funktio: $\phi(n) : \mathbb{N} \to \mathbb{N} : \phi(n) = \#U_n$.

Esimerkki 21. a) Tutkitaan joukkoa $\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$. Nyt $\phi(6) = 2$ ja $U_6 = \{[1], [5]\}$, sillä $5 \cdot 5 = 25 \equiv 1 \pmod{6}$ ja tietysti $1 \cdot 1 = 1$. Muille $a \in \mathbb{Z}_6$ on $\text{syt}(a, 6) \neq 1$.
b) $\phi(8) = 4$ ja $U_8 = \{[1], [3], [5], [7]\}$.

Huomautus 22. Jos n on alkuluku, niin lauseen 19 perusteella $[a] \in U_n$ kaikilla $a \neq 0$ ja $[0] \notin U_n$, joten $\phi(n) = n - 1$.

Seuraavan lauseen todistusta varten tarkistamme, että U_n varustettuna tulolla muodostaa ryhmän:

Lemma 23. *$(U_n, \cdot)$ on Abelin ryhmä.*

Todistus. Kokonaislukujen laskusäännöistä seuraa, että tekijälaskutoimitus "$\cdot$" on sekä assosiatiivinen että kommutatiivinen. Selvästi neutraalialkiolle $[1] \in \mathbb{Z}_p$ pätee $[1] \in U_n$. Myös jokaisella $[a] \in U_n$ on yksikön määritelmän perusteella käänteisalkio $[a]^{-1}$. □

4. Eulerin lause

Yleistetään nyt Fermat'n lause koskemaan muitakin kuin alkulukuja:

Lause 24 (Eulerin lause)**.** *Jos* $\text{syt}(a, n) = 1$ *niin* $a^{\phi(n)} \equiv 1 \pmod{n}$.

Todistus. Lemman 23 perusteella yksiköiden joukko $U_n \subset \mathbb{Z}_n$ muodostaa tulolla varustettuna ryhmän. Koska $\text{syt}(a, n) = 1$, niin lauseen 19 perusteella $[a]$ on yksikkö, siis $[a] \in U_n$. Ryhmän U_n kertaluku on $\phi(n)$, joten Lagrangen lauseen nojalla $[a]^{\phi(n)} = [1]$ kaikilla $[a] \in U_n$, siispä $a^{\phi(n)} = 1 \pmod{n}$. □

Huomautus 25. Fermat'n lause on siis Eulerin lauseen erikoistapaus: Jos n on alkuluku, niin $\text{syt}(a,n) = 1$ kaikilla a, joille $p \nmid a$. Tällöin $[a] \in U_n$ kaikilla a, joille $p \nmid a$. Siten $\phi(n) = n-1$ ja Eulerin lause saa muodon: $a^{n-1} \equiv 1 \pmod{n}$.

Esimerkki 26. a) $\text{syt}(5,6) = 1$ ja $\phi(6) = 2$, joten $5^{\phi(6)} = 5^2 = 25 = 4 \cdot 6 + 1 \equiv 1 \pmod{6}$. Vertaa Fermat'n lauseen tulokseen: $5^{3-1} = 25 \equiv 1 \pmod{3}$
b) $\text{syt}(9,8) = 1$ ja $\phi(8) = 4$, joten $9^4 = 6561 = 1640 \cdot 4 + 1 \equiv 1 \pmod{4}$

5. Eulerin funktion arvo

Kuten edellä todettiin, $\phi(n) = n-1$, jos n on alkuluku. Seuraavaksi todistamme lauseen Eulerin funktion arvolle kaikille kokonaisluvuille n. Tätä varten tarvitsemme muutaman aputuloksen:

Lemma 27. *Jos p on alkuluku ja $n = p^e$, niin*

$$\phi(n) = \phi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1) = n(1 - \frac{1}{p}).$$

Todistus. $\phi(p^e)$ antaa niiden kokonaislukujen a lukumäärän, jotka kuuluvat joukkoon $P := \{1, \ldots, p^e\}$ ja joille lauseen 19 nojalla $\text{syt}(p^e, a) = 1$. Joukossa P on p^e alkiota, joista joka p:nnellä alkiolla on yhteinen tekijä luvun p^e kanssa. Näitä lukuja on $p^e/p = p^{e-1}$ kappaletta, joten $\phi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1)$. □

Lemma 28. *Jos joukko $A = \{1, \ldots, n\}$ on täydellinen jakojäännösten joukko* (mod n) *ja m ja c kokonaislukuja siten, että* $\text{syt}(m,n) = 1$*, niin myös joukko $Am + c := \{am + c \in \mathbb{Z} : a \in A\}$ on täydellinen jakojäännösten joukko* (mod n).

Todistus. Oletetaan, että $am + c \equiv a'm + c \pmod{p}$. Vähentämällä c ja jakamalla m saadaan $a \equiv a' \pmod{n}$ ja $a = a'$, joten jokainen alkio $am + c \in Am + c$ kuuluu eri luokkaan. Koska $\#(Am + c) = n$, niin joukko $Am + c$ on täydellinen jakojäännösten joukko (mod n). □

Lemma 29. *Olkoon $m, n > 1$ ja* $\text{syt}(m,n) = 1$*. Tällöin $\phi(mn) = \phi(m)\phi(n)$.*

Todistus. Jos $a \in U_{mn}$, niin lauseen 19 nojalla $\text{syt}(a, mn) = \text{syt}(a,m) = \text{syt}(a,n) = 1$. Tutkitaan mitkä joukon $\mathbb{Z}_{mn}$ alkioista toteuttavat tämän ehdon: Kirjoitetaan joukon $\mathbb{Z}_{mn}$ alkiot n riviin ja m sarakkeeseen:

$$\begin{array}{llll} 1 & 2 & \ldots & m \\ m+1 & m+2 & \ldots & 2m \\ \vdots & \vdots & & \vdots \\ (n-1)m+1 & (n-1)m+2 & \ldots & nm \end{array}$$

Näin kirjoitettuna sarakkeet muodostavat ekvivalenssiluokat (mod m). Näistä luokista $\phi(m)$ kappaletta sisältää luvut $a \in \mathbb{Z}_{mn}$, joille pätee $\text{syt}(a,m) = 1$. Tämän ehdon toteuttavien sarakkeiden alkiot ovat muotoa $c,\ m+c,\ 2m+c,\ \ldots\ , (n-1)m+c$, joten jokainen tällainen sarake muodostaa lemman 28 nojalla täydellisen jakojäännösten joukon (mod n) ja siten näistä alkioista $\phi(n)$ kappaletta toteuttaa ehdon $\text{syt}(a,n) = 1$. Ehdon $\text{syt}(a, mn) = 1$ toteuttavia alkioita on siis $\phi(m)\phi(n)$ kappaletta.

□

Lause 30. *Olkoon luvulla n alkulukuesitys $n = p_1^{e_1} \cdots p_k^{e_k}$. Tällöin:*

$$\phi(n) = \prod_{i=1}^{k}(p_i^{e_i} - p_i^{e_i-1}) = \prod_{i=1}^{k} p_i^{e_i-1}(p_i - 1) = n\prod_{i=1}^{k}(1 - \frac{1}{p_i}).$$

Todistus. Lemma 27 käsittelee tapauksen $k = 1$, joten tehdään todistus induktiolla kaikille $k > 1$: Oletetaan, että väite pätee kaikilla lukua k pienemmillä kokonaisluvuilla. Koska kaikki $p_i^{e_i}$ ovat keskenään jaottomia, niin lemman 29 perusteella $\phi(n) = \phi(p_1^{e_1} \cdots p_{k-1}^{e_k-1})\phi(p_k^{e_k})$. Lemman 27 perusteella $\phi(p_k^{e_k}) = (p^{e_k} - p^{e_k-1})$ ja induktio-oletuksen mukaan $\phi(p_1^{e_1} \cdots p_{k-1}^{e_k-1}) = \prod_{i=1}^{k-1}(p_i^{e_i} - p_i^{e_i-1})$. Nämä yhdistämällä saadaan:

$$\phi(n) = \prod_{i=1}^{k}(p_i^{e_i} - p_i^{e_i-1}).$$

Muut muodot saadaan helposti kirjoittamalla tulo uudestaan. □

Huomautus 31. Tulos voidaan myös kirjoittaa muodossa:

$$\phi(n) = n\prod_{p|n}(1 - \frac{1}{p}),$$

missä merkintä $\prod_{p|n}$ tarkoittaa, että tulo lasketaan käyden läpi jokainen alkuluku p, joka jakaa luvun n.

Esimerkki 32. a) $9 = 3^2$, joten $\phi(9) = 9 \cdot (1 - \frac{1}{3}) = 6$
b) $14 = 2 \cdot 7$, joten $\phi(14) = 14\prod_{p|14}(1 - \frac{1}{p}) = 14 \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{7}) = 6$

Lause 33.

$$\sum_{d|n} \phi(d) = n$$

Tässä $\sum_{d|n}$ tarkoittaa summaa yli kaikkien lukujen d, jotka jakavat luvun n.

Todistus. Todistus perustuu siihen, että luvut d, jotka jakavat luvun n, osittavat joukon $S = \{1, \ldots, n\}$ alkiot osajoukkoihin $S_d = \{a \in S : \text{syt}(a, n) = \frac{n}{d}\}$. Koska $\text{syt}(a, n)$ jakaa luvun n ja luku on yksikäsitteinen jokaisella $a \in S$, niin osajoukot ovat erillisiä. Riittää siis osoittaa, että osajoukoille pätee $\#S_d = \phi(d)$: Määritellään jokaiselle a luku $a' = a\frac{d}{n}$. Koska $\text{syt}(a, n) = \frac{n}{d} \mid a$ niin a' on kokonaisluku kaikilla a. Tällöin ehdosta:

$$a = a'\frac{n}{d} \in S_d \Longleftrightarrow 1 \leq a'\frac{n}{d} \leq n \; ja \; \text{syt}(a'\frac{n}{d}, n) = \frac{n}{d},$$

saadaan luvulla $\frac{n}{d}$ jakamalla:

$$a \in S_d \Longleftrightarrow 1 \leq a' \leq d \; ja \; \text{syt}(a', d) = 1.$$

Tällaisia lukuja a' on määritelmän mukaan $\phi(d)$. □

Esimerkki 34 ([2] Harjoitus 5.14)**.** Olkoon a luku, jolle $\text{syt}(a, 10) = 1$. Osoitetaan, että kolme viimeistä luvun a^{2001} numeroa ovat samat kuin luvun a. Toisin sanoen, etsitään lukua x, jolle $a^{2001} \equiv x \pmod{1000}$. Oletetaan ensin, että $a > 100$. Koska $\text{syt}(a, 10) = 1$, niin myös $\text{syt}(a, 1000) = 1$, ja siten Eulerin lauseen nojalla: $a^{\phi(1000)} \equiv 1$. Luvun 1000 alkulukutekijät ovat 2 ja 5, joten lause 30 antaa: $\phi(1000) = 1000 \cdot \frac{1}{2} \cdot$

$\frac{4}{5} = 400$. Siis $a^{400} \equiv 1 \pmod{1000}$. Koska $2001 \equiv 1 \pmod{400}$, niin $a^{2001} \equiv a^1 = a \pmod{1000}$. Mikäli $a < 100$, niin helposti huomataan myös, että $a^{2001} \equiv a \pmod{10}$ ja $a^{2001} \equiv a \pmod{100}$, jolloin luvun a^{2001} viimeinen tai viimeiset kaksi numeroa ovat edelleen samat kuin luvun a.

6. Yksiköiden ryhmän U_n syklisyys

Seuraavassa tutkimme ryhmän U_n syklisyyttä, eli millä luvun n arvoilla ryhmä U_n on syklinen. Seuraava esimerkki havainnollistaa, ettei syklisyyden tutkimiseksi riitä ryhmän U_n asteen tietäminen.

Sopimus 35. Merkintöjen yksinkertaistamiseksi merkitään jatkossa luokkaa $[a]$ yksinkertaisesti luvulla a. Jätetään myös merkitsemättä $\pmod{p}$, kun p on yhteydessä selvä ja käytetään yksinkertaisesti merkintää $\equiv$.

Esimerkki 36. a) Ryhmän $U_8 = \{1, 3, 5, 7\}$ aste on 4 ja sen alkioiden asteet 1, 2, 2 ja 2, sillä $1^1 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8}$. Huomataan, että U_8 ei ole syklinen.

b) Ryhmän $U_{10} = \{1, 3, 7, 9\}$ aste on 4. Ryhmän alkioiden asteet ovat vastaavasti 1, 4, 4 ja 2. U_{10} on syklinen, $U_{10} = \langle 3 \rangle = \langle 7 \rangle$, sillä $3^2 \equiv 9$, $3^3 \equiv 7$ ja $3^4 \equiv 1$.

Määritelmä 37. Jos ryhmä U_n on syklinen, niin alkiota $a \in U_n$, joka virittää sen kutsutaan *primitiiviseksi juureksi* $\pmod{n}$.

Primitiivisen juuren $a \in U_n$ aste on siis $\phi(n)$. Kuten edellisessä esimerkissä huomattiin, 3 on primitiivinen juuri (mod 10). Seuraavat lauseet kertovat, millä luvun n arvoilla ryhmällä U_n on primitiivinen juuri ja kuinka monta niitä on:

Lause 38. *Jos p on alkuluku, niin U_p on syklinen ryhmä ja $\phi(p-1)$ antaa sen primitiivisten juurten lukumäärän.*

Todistus. Jotta ryhmä U_p olisi syklinen, on sillä oltava primitiivinen juuri. Fermat'n lauseen nojalla kaikille $a \in U_p$ pätee $a^{p-1} \equiv 1$, ja lisäksi Lagrangen lauseen nojalla $\#a \mid p-1$. Tutkitaan siis alkioita $a \in U_p$, joille $\#a = d \mid p-1$:
Olkoon $\omega(d)$ niiden alkioiden $a \in U_p$ lukumäärä, joiden aste on d. Koska jokaisella alkiolla on jokin aste, niin:

$$\sum_{d \mid p-1} \omega(d) = p - 1.$$

Lisäksi lauseen 33 nojalla:

$$\sum_{d \mid p-1} \phi(d) = p - 1.$$

Riittää siis osoittaa, että $\omega(d) \leq \phi(d)$, jolloin $\omega(d) = \phi(d)$ kaikilla d. Tällöin $\phi(p-1)$ antaa ryhmän U_p primitiivisten juurten lukumäärän.

Oletetaan, että $\omega(d) > 0$ ja että a on astetta d oleva alkio. Koska alkion aste on d, kaikki $a^i = a, a^2, \ldots, a^d$ ovat eri alkioita. Niille pätee $(a^i)^d = 1$, joten ne ovat yhtälön $x^d \equiv 1$ juuria. Tällä yhtälöllä on korkeintaan d ratkaisua (katso [1], Lause 109), joten a^i muodostavat kaikki yhtälön juuret.

Osoitetaan nyt, että astetta d olevat alkiot ovat niitä juuria a^i, joille $\mathrm{syt}(i, d) = 1$:
Olkoon b astetta d oleva alkio. Tällöin b on yhtälön $x^d \equiv 1$ ratkaisu, siis $b = a^i$ jollakin $i = 1, \ldots, d$. Olkoon $\mathrm{syt}(i, j) = k$, jolloin:

$$b^{\frac{d}{k}} = a^{i\frac{d}{k}} = (a^d)^{\frac{i}{k}} = 1^{\frac{i}{k}} \equiv 1,$$

Koska b oli astetta d, on oltava $k = 1$. Täten kaikki alkiot b, jotka ovat astetta d, ovat muotoa a^i, missä $1 \leq i \leq d$ ja $\text{syt}(i, d) = 1$. Tällaisten lukujen i määrä on $\phi(d)$, joten alkioiden b lukumäärä, $\omega(d)$, on $\phi(d)$. □

Huomautus 39. Edellisen todistuksen nojalla, mikäli d jakaa luvun $p-1$, niin ryhmällä U_p on $\phi(d)$ kappaletta alkioita, joiden aste on d.

Esimerkki 40. a) $\phi(5-1) = \phi(4) = 2$. Ryhmällä U_5 on siis kaksi primitiivistä juurta, tarkemmin luvut 2 ja 3.

b) Ryhmällä U_{11} on $\phi(11-1) = \phi(10) = 10 \cdot \frac{1}{2} \cdot \frac{4}{5} = 4$ primitiivistä juurta. Nämä ovat: 2, 6, 7 ja 8. Edellisen huomautuksen nojalla sillä on 1, 1 ja 4 kappaletta alkioita, joiden asteet ovat vastaavasti 1, 2 ja 5.

Seuraava lause kertoo kaikki ne luvun n arvot, joilla U_n on syklinen. Lauseen todistus jätetään tässä työssä laajuutensa vuoksi tarkemmin käsittelemättä, joten toteamme vain:

Lause 41. *Ryhmä U_n on syklinen, jos ja vain jos*

$$n = 1, 2, 4, p^e \text{ tai } 2p^e,$$

missä $p > 2$ on alkuluku.

Todistus. Katso [2] Lause 6.11. □

7. Sovelluksia

Lukuteorian tuloksia sovelletaan nykyisin tiedonsiirron salauksessa. Yksinkertainen keino salata teksti on antaa kirjaimille vastaavat numerot: $A = 0$, $B = 1$, ..., $Z = 25$. Käytämme esimerkeissä siis tietotekniikassa yleistä kirjaimistoa $A - Z$. Kun jokaisella on sitä vastaava luku, merkitään tätä lukua jatkossa x, jokaiseen lukuun lisätään jokin luku k (niin sanottu "key") ja lasketaan uudelleen jokaista kirjainta vastaava luku (mod 26) ja edelleen sitä vastaava kirjain. Nyt jokaisella kirjaimella on täsmälleen yksi sitä vastaava kirjain: $x \mapsto x + k \pmod{26}$. Alkuperäinen teksti saadaan palautettua salatusta käänteisellä operaatiolla vähentämällä k jokaista kirjainta vastaavasta luvusta.

Esimerkki 42. Olkoon $k = 3$. Tällöin nimi JUHANI muuttuu edellä esitellyllä menetelmällä kirjainsarjaksi MXKDQL.

Tällainen salaus on tietenkin helppo purkaa arvaamalla luku k esimerkiksi kielen useimmin esiintyvien kirjainten perusteella tai käymällä läpi kaikki 26 (käytännössä 25) mahdollista luvun k arvoa. Vahvempi salaus saadaan käyttämällä muunnosta: $x \mapsto ax + b \pmod{26}$. Jotta muunnos olisi yksikäsitteinen, on a oltava yksikkö (mod 26). Mahdollisten muunnosten lukumäärä saadaan tällöin laskemalla $\phi(26) \cdot 26 = \phi(2) \cdot \phi(13) \cdot 26 = 12 \cdot 26 = 312$. Tällaisen salauksen purkaminen ei edelleen ole tietokoneelle ongelma.

Esimerkki 43. Olkoon $a = 3$ ja $b = 2$. Tällöin nimi JUHANI muuttuu kirjainsarjaksi DKXCPA.

Edelleen vahvempi salausmenetelmä saadaan hyödyntämällä Fermat'n pientä lausetta: Valitaan suuri alkuluku p ja luku e, jolle $\text{syt}(e, p-1) = 1$. Nyt muunnoksena käytetään: $x \mapsto x^e \pmod{p}$. Salauksen purkamiseksi etsitään luku f, jolle

$ef \equiv 1 \pmod{p-1}$. Koska $\text{syt}(e, p-1) = 1$, e on yksikkö (mod $p-1$) ja tällainen f on mahdollista löytää. Tällöin $ef = (p-1)k + 1$, jollakin kokonaisluvulla k, joten Fermat'n lauseen nojalla:

$$(x^e)^f = x^{(p-1)k+1} = x \cdot (x^{p-1})^k \equiv x \pmod{p}$$

Alkuperäinen luku x saadaan siis selvitettyä yksinkertaisesti korottamalla x^e potenssiin f.

Kuten edellä mainittiin, salauksen purkamisessa voidaan hyödyntää tietoa kielen useimmin esiintyvistä kirjaimista. Tämä voidaan estää jakamalla teksti k kirjaimen pituisiin osiin ja valitsemalla niin iso p, että jokainen erilainen osa voidaan esittää eri luokkana $x \pmod{p}$. Näin saatuun lukuun x sovelletaan edellistä menetelmää. Tällä tavoin salatun tekstin purkaminen tietämättä lukua f osoittautuu vaikeaksi jopa tietokoneelle.

Ongelma tällaisessa menetelmässä on, kuinka lähettäjä ja vastaanottaja voivat sopia lukujen p ja e arvot (näitä lukuja kutsutaan *avaimeksi*) siten, ettei kukaan muu saa niitä tietoonsa. Tämä voidaan kiertää käyttämällä erästä *julkisen avaimen menetelmää*: Olkoon systeemissä käyttäjät vastaanottaja ja lähettäjä. Mikäli vastaanottaja haluaa lähettäjän siirtävän hänelle tietoa salatussa muodossa, hän ottaa kaksi suurta alkulukua p ja q ja laskee luvun $pq = n$. Osoittautuu, että jos luvut p ja q ovat tarpeeksi suuria, luvun n jakaminen tekijöihin on käytännössä ajallisesti mahdotonta. Nyt ainoastaan vastaanottajan on helppo laskea lemman 29 avulla luku $\phi(n) = (p-1)(q-1)$. Vastaanottaja pitää tämän luvun salaisena ja etsii luvun e, jolle $\text{syt}(\phi(n), e) = 1$ ja julkaisee koko systeemille luvut e ja n, joita kutsutaan *julkiseksi avaimeksi*. Nyt lähettäjä ottaa tämän julkisen avaimen ja salaa viestin käyttäen muunnosta: $x \mapsto x^e \pmod{n}$. Koska $\text{syt}(\phi(n), e) = 1$, vastaanottajan on helppo etsiä f, jolle $ef \equiv 1 \pmod{\phi(n)}$. Kunhan $\text{syt}(x, n) = 1$, siis $x \neq kp$ ja $x \neq kq$ kaikilla $k \in \mathbb{N}$, niin Eulerin lauseen nojalla: $(x^e)^f \equiv x \pmod{n}$. Vastaanottaja voi siis purkaa salauksen helposti potenssiinkorotuksella.

Salauksen turvallisuus perustuu siihen, että vaikka salakuuntelijalla olisi nyt tiedossa yhtälöstä $(x^e)^f \equiv x \pmod{n}$, luvut x, e ja n, ei luvun f ratkaisemiseen ole tehokasta algoritmia. Tämän takia valitaan suuret arvot luvuille p ja q, jolloin yhtälön ratkaiseminen mielekkäässä ajassa ei ole mahdollista. Potenssiinkorotus sen sijaan on tietoteknisesti yksinkertainen operaatio, jos f on tiedossa.

Tämä menetelmä mahdollistaa myös viestin allekirjoittamisen ja siten lähettäjän varmistamisen: Ensin lähettäjä salaa oman nimensä käyttäen omia lukuja n ja f, joista f on vain hänen tiedossa. Seuraavaksi hän salaa saamansa tuloksen käyttäen vastaanottajan julkista avainta, n ja e, ja lähettää viestin. Nyt vastaanottaja purkaa viestin käyttäen omia lukujaan n ja f ja uudelleen purkaa tämän tuloksen käyttäen lähettäjän julkista avainta, n ja e. Nimelle on siten tehty kaksi paria käänteisiä operaatiota, joten vastaanottajalla pitäisi olla lähettäjän nimi. Koska vain lähettäjä tietää luvun f, vain hän on voinut tehdä ensimmäisen operaation oikein, ja vastaanottaja voi olla varma lähettäjästä.

Esimerkki 44. Tutkitaan edellä esitettyä allekirjoitusmenetelmää: Olkoon lähettäjän luvut f_1, n_1 ja e_1 ja vastaanottajan luvut f_2, n_2 ja e_2. Lähettäjä salaa oman nimensä:

$$x \mapsto x^{f_1} \pmod{n_1}$$

ja salaa tuloksen käyttäen vastaanottajan julkista avainta:

$$x^{f_1} \mapsto (x^{f_1})^{e_2} \pmod{n_2}.$$

Vastaanottaja purkaa viestin käyttäen omia lukujaan:

$$(x^{f_1})^{e_2} \mapsto \left((x^{f_1})^{e_2}\right)^{f_2} \equiv x^{f_1} \pmod{n_2}$$

ja purkaa sen uudestaan käyttäen lähettäjän julkista avainta:

$$x^{f_1} \mapsto (x^{f_1})^{e_1} \equiv x \pmod{n_1}.$$

Kirjallisuutta

[1] Hardy, G. H. & Wright, E. M.: *An introduction to the theory of numbers,* Oxford university press, US 2008.
[2] Jones, Gareth A. & J. Mary: *Elementary number theory,* Springer-Verlag, UK 2005.